PCT/EP 99/00283

09/600121

Europäisches Patentamt | European Patent Office | Office européen des brevets

5

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

98200081.2

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

Arlette Fiedler

A. Fiedler

DEN HAAG, DEN
THE HAGUE, 24/[illegible]/99
LA HAYE,

[illegible] 1014 - 02.91

Europäisches Patentamt | European Patent Office | Office européen des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.: Application no.: Demande n°: 98200081.2

Anmeldetag: Date of filing: Date de dépôt: 14/01/98

Anmelder: Applicant(s): Demandeur(s):
IRDETO B.V.
2132 HD Hoofddorp
NETHERLANDS

Bezeichnung der Erfindung: Title of the invention: Titre de l'invention:
Method for transferring data from a head-end to a number of receivers

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat: State: Pays:	Tag: Date: Date:	Aktenzeichen: File no. Numéro de dépôt:

Internationale Patentklassifikation: International Patent classification: Classification internationale des brevets:
H04L29/06

Am Anmeldetag benannte Vertragstaaten: Contracting states designated at date of filing: AT/BE/CH/[redacted]/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE
Etats contractants désignés lors du depôt:

Bemerkungen: Remarks: Remarques:

Method for transferring data from a head-end to a number of receivers

The present invention relates to a method for transferring data from a head-end to a number of receivers by means of a digital broadcast signal, each of said receivers including a descrambler for descrambling a received digital transport stream.

The use of a digital broadcast signal, such as a DVB signal, for transferring data to one or more receivers shows the advantage that available receivers with descramblers can be used to transfer the data from a head-end to the receiver. However, such a method would normally not allow for a data transfer in a secure and private manner as the data is accessible to all receivers listening to the digital transport stream.

The present invention aims to provide a method of the above-mentioned type wherein privacy and security of the data transfer can be provided to each receiver.

According to the invention a method of the above-mentioned type is provided, including the steps of one or more receivers receiving data packets, sending a message with a unique key from the head-end to said one or more receivers, loading the unique key in the descrambler of the respective receivers, providing a table of unique keys with corresponding addresses at the head-end, providing data packets with an individual address of said one or more receivers, inserting said data packets into a transport packet of a digital transport stream, selecting a key from said table in accordance with the address of the data packet, scrambling said transport packet using the selected key and descrambling the transport stream using the unique key at the receiver having this unique key.

In this manner a method is obtained wherein each receiver attempting to descramble the broadcast signal will

through the head-end 1 by means of a broadcast signal in the following manner.

The IP data includes an IP or MAC address of the receiver 2 requesting the data to be transferred to this receiver. Each receiver 2 for which the head-end 1 receives IP data packets with an individual address, i.e. the IP or MAC address, is sent a so-called Entitlement Control Message or ECM with a control word or key which is unique to the receiver 2. At the head-end 1 the unique keys with the corresponding individual addresses are stored in a table 6. At the receiver(s) 2 to which an ECM is sent, the smart card 4 decrypts the unique key as it would do for a normal subscription service. The decrypted key is loaded into the descrambler 3 for future use.

At the head-end 1, the IP data packets for a specific receiver 2 requesting IP data, are inserted into a transport packet of the MPEG transport stream. Before scrambling the transport packet containing the IP data packets, the headend checks the IP or MAC address and selects the corresponding unique key from the table 6, which key is used to scramble the transport packet.

Each receiver 2 listening to the digital broadcast signal attempts to descramble the signal, wherein however only at the receiver 2 having the unique key the descrambling process will be successful. In this manner only one receiver 2 will descramble the IP data packets and will provide this data packets for further processing.

From the above it will be clear that the described method results in a transfer of data with privacy and security for each receiver 2 requesting a data transfer. Moreover, this transfer with privacy and security is achieved while using existing DVB or MPEG scrambling and descrambling equipment.

Generally, a number of receivers 2 will request the transfer of data. This is no problem as the head-end will provide a table 6 including key/address combinations for each receiver 2 requesting a data transfer. The capacity of

CLAIMS

1. Method for transferring data from a head-end to a number of receivers by means of a digital broadcast signal, each of said receivers including a descrambler for descrambling a received digital transport stream, said method including the steps of one or more receivers receiving data packets, sending a message with a unique key from the head-end to said one or more receivers, loading the unique key in the descrambler of the respective receivers, providing a table of unique keys with corresponding addresses at the head-end, providing data packets with an individual address of said one or more receivers, inserting said data packets into a transport packet of a digital transport stream, selecting a key from said table in accordance with the address of the data packet, scrambling said transport packet using the selected key and descrambling the transport stream using the unique key at the receiver having this unique key.

2. Method according to claim 1, wherein for transferring data packets to two or more receivers, the data packets for different receivers are inserted into different transport packets, each of said transport packets being scrambled with a unique key corresponding with the individual address of the corresponding data packets.

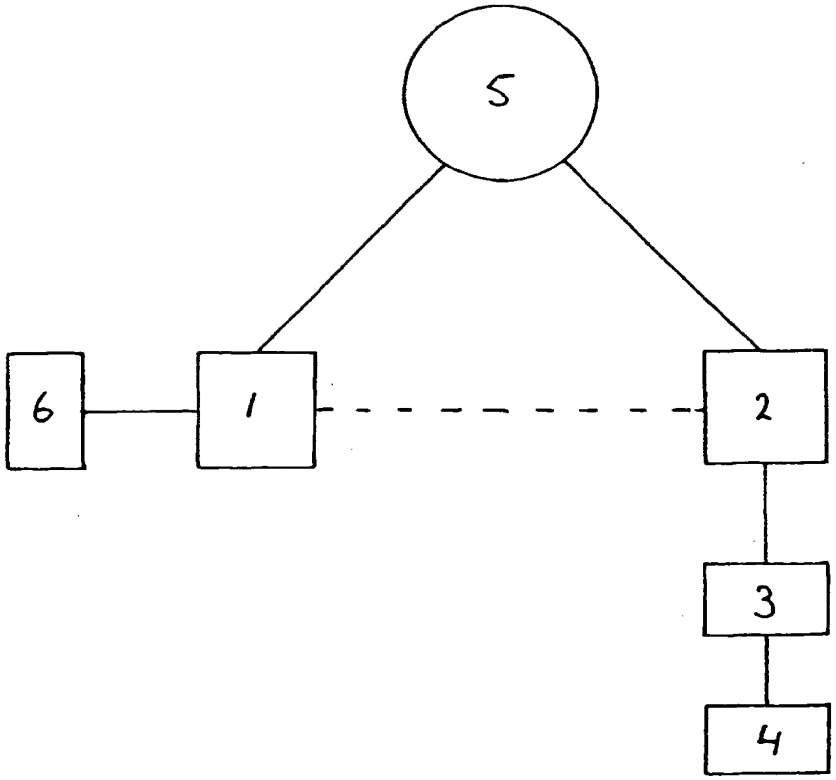
3. Method according to claim 1 or 2, wherein each receiver is adapted to request the transfer of specific data from the head-end.

4. Method according to claim 1, 2 or 3, wherein the data packets to be transferred are IP data packets.

H 14.01.99

ABSTRACT

A method for transferring data from a head-end to a number of receivers by means of a digital broadcast signal is described, wherein each of the receivers includes a descrambler for descrambling a received digital transport stream. The method includes the steps of one or more receivers receiving data packets, sending a message with a unique key from the head-end to said one or more receivers, loading the unique key in the descrambler of the respective receivers, providing a table of unique keys with corresponding addresses at the head-end, providing data packets with an individual address of said one or more receivers, inserting said data packets into a transport packet of a digital transport stream, selecting a key from said table in accordance with the address of the data packet, scrambling said transport packet using the selected key and descrambling the transport stream using the unique key at the receiver having this unique key.


5
6
1
2
3
4